대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2002-0072813
Application Number

출 원 년 월 일 : 2002년 11월 21일
Date of Application NOV 21, 2002

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2003 년 11 월 07 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2002.11.21
【발명의 명칭】	멀티미디어 데이터 암호화 압축방법 및 장치
【발명의 영문명칭】	CODING COMPRESSION APPARATUS AND METHOD FOR MULTIMEDIA DATA
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	김동진
【대리인코드】	9-1999-000041-4
【포괄위임등록번호】	2002-007585-8
【발명자】	
【성명의 국문표기】	조성연
【성명의 영문표기】	CHO,Song Yean
【주민등록번호】	750930-2057121
【우편번호】	156-011
【주소】	서울특별시 동작구 신대방1동 경남교수아파트 103-1704
【국적】	KR
【발명자】	
【성명의 국문표기】	문병인
【성명의 영문표기】	MUN,Byung In
【주민등록번호】	670210-1411225
【우편번호】	442-706
【주소】	경기도 수원시 팔달구 망포동 동수원엘지빌리지 104-1401
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 김동진 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	7	면	7,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	7	항	333,000 원
【합계】	369,000 원		

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 멀티미디어 데이터를 기록 및 전송하기 위해 압축하는 과정에서 소정의 암호화키를 통해 멀티미디어 데이터를 변환하여 압축함으로써 압축하는 과정에서, 사용된 암호화키를 이용해야만 복호화가 가능하도록 암호화하는 멀티미디어 데이터 암호화 압축방법 및 장치를 개시한 것이다.

본 발명에 따른 멀티미디어 데이터 암호화 압축방법은 입력되는 멀티미디어 데이터를 DCT에 적용시켜 DCT 계수를 생성하고, 생성된 DCT 계수를 양자화하는 단계와; 양자화된 DCT의 DC 및 AC 계수를 엔트로피 인코딩할 때 소정의 암호화키에 따라 인코딩 결과를 변환시켜 변환된 DC 및 AC 계수를 암호화하는 단계와; 암호화된 DC 및 AC 계수를 허프만 테이블을 통해 허프만 부호화하여 출력하는 단계로 이루어지는 것으로서, 이를 통해 무선 통신 상의 멀티미디어 데이터 처리에 알맞는 압축방법을 제공한다.

【대표도】

도 3

【색인어】

MPEG, 멀티미디어, 암호화

【명세서】

【발명의 명칭】

멀티미디어 데이터 암호화 압축방법 및 장치{CODING COMPRESSION APPARATUS AND METHOD FOR MULTIMEDIA DATA}

【도면의 간단한 설명】

도 1은 종래의 MPEG 압축 기법을 이용하는 멀티미디어 데이터를 DES를 통해 암호화하기 위한 장치의 개략적인 구성을 나타낸 것이다.

도 2는 종래의 MPEG 압축 기법을 이용하는 멀티미디어 데이터를 DES를 통해 암호화하는 개략적인 시스템 구성을 나타낸 것이다.

도 3은 본 발명에 따른 멀티미디어 암호화 압축장치의 개략적인 구성을 나타낸 것이다.

도 4는 본 발명에 따른 멀티미디어 암호화 압축방법의 동작 과정을 나타낸 것이다.

도 5는 본 발명에 따른 멀티미디어 암호화 압축장치를 포함하는 개략적인 시스템 구성을 나타낸 것이다.

도 6의 a내지 c는 본 발명에 따른 원본 이미지 및 암호화 압축한 결과를 나타낸 것이다.

도 7의 a내지 c는 본 발명에 따른 또 다른 원본 이미지 및 암호화 압축한 결과를 나타낸 것이다.

* 도면의 주요부분에 대한 부호의 설명 *

110 : 이산 여현 변환부(DCT) 130 : 양자화 테이블

150 : 양자화부 170 : 엔트로피 암호화 인코딩부

171 : DPCM 173 : Run Length 부호화부

175 : 암호화부 177 : 허프만 테이블

179 : 허프만 부호화부

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<14> 본 발명은 멀티미디어 데이터 암호화 압축방법 및 장치에 관한 것으로서, 특히 멀티미디어 데이터를 기록 및 전송하기 위해 압축하는 과정에서 소정의 암호화키를 통해 멀티미디어 데이터를 변환하여 압축함으로써 압축하는 과정에서 사용된 암호화키를 이용해야만 복호화가 가능하도록 암호화하는 멀티미디어 데이터 암호화 압축방법 및 장치에 관한 것이다.

<15> MPEG(Moving Picture Expert Group)은 동화상 및 오디오의 압축 저장 및 전송을 비롯하여 압축된 정보의 복원, 처리 및 부호화 표현 방법에 대한 국제 표준안이다.

<16> MPEG 표준은 MPEG 1, MPEG 2, MPEG 4가 있는데, 이 가운데 멀티미디어 데이터의 가장 기본이 되는 MPEG-1(ISO/CEI 11172)은 중복된 정보를 제거하거나 변환시키고 거기에 통계적 특성을 적용하여 동영상 신호를 압축하는 것이다.

<17> 이러한 MPEG에서는 공간적인 중복성을 제거하기 위한 수단으로 이산 여현 변환(Discrete Cosine Transform: 이하, DCT라 칭함)과 양자화(Quantization)를 사용하고, 시간적 중복성을 제거하기 위해 DPCM(Differential Pulse Code Modulation)을 사용하고 있으며, 추가적으로 런 길이 부호화(Run Length Coding) 및 허프만 부호화(Huffmann Coding)로 이루어지는 엔트로피 부호화(entropy encoding)를 사용하고 있다.

<18> 또한, MPEG은 기본적으로 다수의 프레임(frame) 집합인 GOP(Group of Picture)들로 구성되어 있으며, 각 GOP는 I-frame(Intra frame), P-frame(forward-predicted frame), B-frame(bi-directional predicted frame)들로 구성된다.

<19> 최근, 무선 통신 기술의 발달과 이동 통신이 폭 넓게 제공되면서 이러한 압축 기술을 기반으로 하는 무선 네트워크 상에서의 멀티 미디어 서비스가 활성화되고 있는데, 이에 따라 멀티 미디어 서비스를 통해 제공하는 데이터에 대한 보완성이 더욱 요구되고 있다.

<20> 즉, 서비스 이용권한이 있는 사용자에게만 해당되는 서비스를 제공하는 것으로, 일예로, 일정 사용요금을 지불한 사용자들에게만 영화를 전송한다거나, 기밀 회의에 참여할 권한이 있는 사용자에게만 화상 정보를 전송하는 것이다.

<21> 이러한 보안성을 제공하기 위한 암호화 알고리즘으로는 1997년 국제표준 알고리즘으로 채택된 데이터 암호화 표준(Data Encryption Standard: 이하, DES라고 칭함)이 주로 사용되고 있다.

<22> DES는 대칭키(symmetric key)를 사용하여 블록 단위의 평문(plain text)을 처리하는 블록 암호 알고리즘인데, 보안성 있는 멀티미디어 서비스를 위해 압축된 멀티미디어 데이터를 전송 및 재생하기 위해서도 사용되고 있다.

<23> 이와 같이, MPEG 압축 기법을 이용하는 멀티미디어 데이터를 암호화 하는 방법에 관하여 앞서 제안된 바 있는, 미국특허 제 6021199 호(발명의 명칭: Motion picture data encrypting method and computer system and motion picture data encoding/decoding apparatus to which encrypting method is applied')는 원 화상 정보를 모두 담고 있는 I-frame의 특성을 이용하여

MPEG 데이터 중에서 I-frame만을 DES를 사용하여 선택적으로 암호화(encryption)하여 데이터 양을 줄인다.

<24> 이러한 MPEG 압축 기법을 이용하는 멀티미디어 데이터를 암호화 하는 과정은 첨부된 도 1과 2에 나타낸 바와 같이 이루어진다.

<25> 즉, 도 1에 도시한 바와 같이, DCT와 양자화 과정을 거치면서 입력된 8×8 블록 내의 많은 값들이 0이 된다.

<26> 이렇게 처리된 프레임 데이터를 효율적으로 처리하기 위해 DC 계수와 AC 계수 값을 zig-zag 순서에 따라 (DC, AC1, AC2,...AC63)로 읽고, 엔트로피 부호화 과정을 거쳐서 압축하고(100), DES 암호화 과정을 통하여 암호화 처리한다(200).

<27> 또한, 도 2에 도시한 바와 같이, 멀티미디어 데이터 제공자(Multimedia data producer)는 멀티미디어 데이터 수신자(Multimedia data receiver)들로부터 전송되는 공용키(public key)를 수신하고(1), 멀티미디어 서비스를 통해 제공되는 암호화된 멀티미디어 데이터를 복호화하기 위하여 필요한 대칭키를 생성하여 생성된 대칭키를 수신자로부터 받은 공용키로 암호화한 후 수신자에게 전송한다(2).

<28> 그리고, 제공자는 DES에 사용되는 대칭키를 주기적으로 변환함으로써 보완성을 높인다(3).

<29> 이러한 공유된 symmetric key를 사용하여 MPEG 데이터를 DES 알고리즘에 따라 암호화하는 방식은 암호화 및 복호화 과정이 복잡하기 때문에 암호화 및 복호화 과정을 처리하기 위한 리소스가 요구된다.

<30> 또한, 멀티미디어 압축률을 향상시키지 못하기 때문에, 무선 이동 단말기를 대상으로 하는 실시간 멀티 미디어 서비스에는 부적합하였다.

<31> 따라서, 무선 네트워크 환경의 대역폭(bandwidth)자원과 이동 단말기의 연산(computation) 자원의 한계를 효율적으로 사용할 수 있는 멀티 미디어 보안 시스템이 요구되고 있는 실정이다.

【발명이 이루고자 하는 기술적 과제】

<32> 본 발명은 상기한 종래 기술의 문제점을 보완하기 위하여 안출된 것으로, MPEG 압축 과정에서 엔트로피 인코딩을 수행할 때 소정의 암호화키에 따라 엔트로피 인코딩함으로써 변환되는 인코딩 결과에 따라 멀티미디어 데이터를 암호화하고 압축하는 것을 목적으로 한다.

<33> 본 발명의 다른 목적은 소정의 대칭 키를 이용한 부호화 과정을 통해 압축 효율을 증대시키는 것을 목적으로 한다.

【발명의 구성 및 작용】

<34> 이하, 본 발명에 따른 멀티미디어 암호화 압축방법 및 장치를 첨부된 도면을 참조하여 상세히 설명한다.

<35> 본 발명에 따른 멀티미디어 암호화 압축방법은 입력되는 멀티미디어 데이터를 DCT에 적용시켜 DCT 계수를 생성하고, 생성된 DCT 계수를 양자화하는 단계와; 양자화된 DCT의 DC 및 AC 계수를 엔트로피 인코딩할 때 소정의 암호화키에 따라 인코딩 결과를 변환시켜 변환된 DC 및 AC 계수를 암호화 압축하는 단계와; 암호화된 DC 및 AC 계수를 허프만 테이블을 통해 허프만 부호화하여 출력하는 단계를 포함하는 것을 특징으로 한다.

<36> 또한, 본 발명에 따른 멀티미디어 암호화 압축장치는 입력되는 멀티미디어 데이터를 이산 신호로 변환하여 AC 및 DC 계수로 이루어지는 DCT 계수를 생성하는 DCT와, DCT 계수를 양자화 테이블을 사용하여 양자화하는 양자화부와, 양자화된 AC 및 DC 계수를 소정의 암호화키를 이용해 엔트로피 인코딩하여 AC 및 DC 계수를 암호화하는 엔트로피 암호화 인코딩부를 포함하는 것을 특징으로 한다.

<37> 먼저, 본 발명에 따른 암호화 압축방법 및 장치는 MPEG-1의 H.261 동화상 압축 알고리즘을 기반으로 구현되는 것으로, 압축 과정을 설명하기 위한 용어의 의미, 계층적 구조 등은 MPEG-1의 동화상 압축 알고리즘에 정의되어 있다.

<38> 따라서, 본 발명에 따른 암호화 압축방법 및 장치를 설명하는데 있어서, 본 발명의 요지를 흐릴 수 있다고 생각되는 용어의 의미, 계층적 구조, 각종 파라미터에 관한 상세한 생략한다.

<39> 또한, 본 발명에서는 symmetric key 값을 이용하여 DC와 AC를 다른 방법으로 암호화하고 있는데, DC는 shi와 Bhargaca의 An Efficient MPEG Video Encryption Algorithm에 제시된 것과 같이 암호키에 따라 부호를 바꾸는 방법을 사용하고, AC는 lossy compression을 추가적으로 하는 방법을 사용하고 있다.

<40> 우선, 본 발명에 따른 암호화 압축장치를 첨부된 도 3을 참조하여 상세히 설명한다.

<41> 도 3에 도시된 바와 같이, 본 발명에 따른 암호화 압축장치는 입력되는 멀티미디어 데이터를 이산 신호로 변환하여 AC 및 DC 계수로 이루어지는 DCT 계수를 생성하는 DCT(110)와, 양자화 테이블(130)을 이용하여 생성된 DCT 계수를 양자화하는 양자화부(150)와, 양자화된 AC 및

DC 계수를 소정의 암호화키를 이용해 엔트로피 인코딩하여 AC 및 DC 계수를 암호화하는 엔트로피 암호화 인코딩부(170)로 구성된다.

<42> 엔트로피 암호화 인코딩부(170)는 DCT 계수의 DC를 펄스 변조하는 DPCM(171)과, DCT 계수의 AC를 zig-zag run으로 스캔하는 런 랭스 부호화부(173)와, DPCM(171)과 런 랭스 부호화부(173)를 통해 얻어지는 DC 및 AC의 VLC 및 VLI를 이용하여 DC 및 AC를 암호화하는 암호화부(175)와, 암호화된 DC 및 AC를 허프만 테이블(177)을 통해 허프만 부호화하는 허프만 부호화부(179)로 구성된다.

<43> 이와 같이 구성되는 암호화 압축장치를 이용하여 멀티미디어 데이터를 암호화 압축하는 방법은 입력되는 멀티미디어 데이터를 DCT(110)에 적용시켜 DCT 계수를 생성하고, 생성된 DCT 계수를 양자화하는 단계와; 양자화된 DCT의 DC 및 AC 계수를 엔트로피 인코딩할 때 소정의 암호화키에 따라 인코딩 결과를 변환시켜 변환된 DC 및 AC 계수를 암호화하는 단계와; 암호화된 DC 및 AC 계수를 허프만 테이블(177)을 통해 허프만 부호화하여 출력하는 단계로 이루어진다.

<44> 암호화하는 단계는 DC 및 AC 계수에서 DC 계수는 DPCM하고 AC 계수는 런 랭스 코드화하는 단계; DPCM 및 런 랭스 코드화과정을 통해 얻어지는 상기 DC 및 AC 계수의 가변 길이 정보(VLC,VLI)를 이용하여 상기 AC 및 DC의 암호화 키 및 암호화키의 시작 비트를 의미하는 랜덤 상수(r)를 결정하는 단계; 결정된 암호화키를 이용해 상기 AC 및 DC 계수를 암호화하는 단계로 이루어진다.

<45> DC 계수를 암호화하는 단계는 결정된 DC의 암호화 키에서 상기 r번째 비트값이 1인지 여부를 판별하는 단계; 판별결과 1이면 상기 DC 계수의 VLC값을 11111111과 배타적 논리합하여 상기DC 계수를 변환시키는 단계를 포함하는 것을 특징한다.

<46> AC 계수를 암호화하는 단계는 결정된 암호화 키에서 상기 r번째 비트값이 1인지 여부를 판별하는 단계; 판별결과 1이면 상기 AC 계수의 VLI를 오른쪽 편이(right shift)시키는 단계; 오른쪽 편이된 VLI값을 통해 허프만 테이블을 이용하여 VLC를 결정하는 단계; 결정된 VLC와 상기 VLI를 이용하여 상기 AC 계수를 변환시키는 단계로 이루어진다.

<47> 상기 암호화키는 두 개의 대칭형 키이며 각각 상기 DC 및 AC의 VLC인 것으로, DC 및 AC의 VLC에 따라 DC 및 AC를 엔트로피 인코딩하여 변화되는 DC 및 AC 인코딩결과 값을 압축함으로써 VLC을 통해서만 디코딩할 수 있도록 하는 것이다.

<48> 이와 같이 이루어지는 본 발명에 따른 멀티미디어 암호화 압축방법을 첨부된 도면을 참조하여 일 실시 예로 상세히 설명한다.

<49> 먼저, 일 예로, zig-zag 순서에 따른 (DC, AC1, AC2, ...AC63)의 벡터 형태가 아래 표 1과 같다면,

<50> 【표 1】

3	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	7	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

<51>

【표 2】

Range of DIFF(k) value	bit size(m)	Huffman code
0	0	00
-1,1	1	010
-3,-2,2,3	2	011
-7,...-4,4,...7	3	100
.....		
-255,...-128,128,...255	8	1111110

<52> 이러한, 8×8 블록을 differential DC와 AC 계수들로 zig-zag 스캔하고, 이를 허프만 테이블을 이용하여 differential DC 및 AC 계수를 표현하기 위한 최소 비트(bit) 수를 나타내는 VLC(Variable Length Coding)과 differential DC에서 VLC 비트 만큼을 취한 VLI(Variable Length Integer)로 인코딩한다.

<53> 상기 예에 따르면, DC 계수는 3 이므로, 표 2(Huffman Code for differential DC) 를 참조하여 3을 표현하기 위한 최소 비트수를 결정하면 2가 된다.

<54> 이에 따라, DC 계수의 VLC=2(011)이고, DC 계수인 3을 표현하는 011의 least significant bit를 VLC 비트(2)만큼을 추출하는 VLI는 11이 된다.

<55> 또한, VLC 및 VLI로 이루어지는 DC 계수의 엔트리피 인코딩 결과는 01111이 된다.

<56> 그리고, AC 계수는 AC 계수는 런 랭스 부호화로 일련의 (0의 반복횟수(I), 0이 아닌 수를 나타내기 위한 비트수(m))가 압축된 비트 스트림이 되는데, 상기 실시 예에 따르면 0의 반복횟수(I)는 7이고 0이 아닌 수 7을 표현하기 위한 비트수는 아래 표. 3(AC coefficient magnitude category for bit size table)을 참조하면 3이므로, (7,3)이 된다.

<57> 【표 3】

Bit size	AC coefficient value range
0	0
1	-1,1
2	-3,-2,2,3
3	-7,...-4,4,..7
4	-15,...-8,8,....15
10	-1023,....-512,512,...1023

<58> 【표 4】

run/level	bits	VLC
7/1	8	11111010
7/2	12	111111111011
7/3	16	1111111111010110
7/4	16	1111111111010111
7/5	16	1111111111011000
7/6	16	1111111111011001
7/7	16	1111111111011010
7/8	10	1111111111011011
7/9	16	1111111111011100
7/A	16	1111111111011101

<59> 이에 따라, 표.4(Typical AC Huffman Code Table)를 이용하여 (7,3)에 해당되는 VLC를 결정하면, AC의 VLC=1111111110101110이다.

<60> 그리고, VLC에서 7을 표현하기 위한 비트수(3)을 취하는 VLI=110이 되므로, VLC 및 VLI로 이루어지는 AC 계수의 엔트리피 인코딩 결과는 11111111110101110110이 된다.

<61> 이러한 과정에 따라, 엔트로피 암호화 인코딩부(170)의 DPCM(171), 런 랭스 부호화부(173)를 통해 DC 및 AC 계수의 VLC 및 VLI가 생성되면, 이를 이용하여 암호화 압축 과정을 수행한다.

<62> DC 및 AC의 VLC 및 VLI를 이용한 암호화 압축 과정을 첨부된 도 4를 참조하여 일 실시예로 설명한다.

<63> 도 4에 도시된 바와 같이, 양자화된 DC 및 AC 계수를 DPCM(171), 런 랭스 부호화(173)하여 각각의 VLC 및 VLI를 생성하고, 생성된 DC 및 AC의 VLC 및 VLI를 이용하여 암호화 키(이하, symmetric key 1, 2로 칭함) 및 암호화 키의 시작 비트를 나타내는 임의의 랜덤 상수(r)를 결정한다(S1).상기 symmetric key 1, 2는 DC 및 AC의 VLC로 결정되는데, key 1은 DC, key 2는 AC로 정의한다.

<64> 이와 같이 symmetric key 1, 2 및 랜덤 상수가 결정되면, DC 계수인지 여부를 판별하여(S2) DC 계수와 AC 계수를 각가 암호화 압축 처리한다.

<65> 판별결과 DC 계수이면, symmetric key 1에서 지정된 랜덤 상수에 해당되는 비트가 1인지 여부를 판별하여(S3), 1이면 DC의 VLI를 11111111과 배타적 합(XOR)한다(S4).

<66> 11111111과의 배타적 합에 의해 VLI 값이 달라짐에 따라 DC 엔코딩 값을 변환한다(S5).

<67> 즉, 랜덤상수를 2이라고 가정하고, 상기 실시 예에 적용하면, VLC=011이고, VLI=11인 DC 계수에서 VLI의 두번째 비트열이 1이기 때문에, 11111111과 배타적 합을 한 결과는 11111100이 된다.

<68> 이와 같은 배타적 합 결과에서 VLC 비트(2)만큼을 추출하는 VLI는 00이 된다.

<69> 상기 달라지는 VLI값에 의해 DC 인코딩 값은 01100으로 변화된다.

<70> 판별결과 DC 계수가 아니면, symmetric key 2에서 지정된 랜덤 상수에 해당되는 비트가 1인지 여부를 판별하여(S6), 1이면 AC의 VLI를 오른쪽으로 편이시킨다(S7).

<71> 오른쪽으로의 편이에 의해 VLI 값이 달라짐에 따라 AC 엔코딩 값을 변환한다(S8).

<72> 즉, 상기 실시 예에 따라 VLC=1111111110101110이고, VLI=110인 AC 계수에서 VLI의 두 번째 비트열이 1이기 때문에, VLI(110)를 오른쪽으로 편이시키면 VLI=011이 된다.

<73> 이와 같이 편이시킨 결과, VLI 값이 3(011)이므로 3을 표현하기 위한 최소비트 2를 AC 계수에 적용하여 AC 계수 (7,3)을 (7,2)로 변환한다.

<74> 이에 따라, (7,2)에 해당되는 VLC를 표 4에서 검색하면 VLC는 1111111110111이 되고, VLC에서 최소 비트수만을 추출하는 VLI는 11이 된다.

<75> 상기 달라지는 VLI에 의해 변화되는 AC 인코딩 값은 111111110111111이 된다.

<76> 이와 같이, 압축된 AC 및 DC 계수는 암호화키인 symmetric key 1, 2를 통해서만 복호화 할 수 있게 됨으로써 암호화 된다.

<77> 이러한 과정을 통해 암호화 키(symmetric key 1, 2)가 결정되고, 멀티미디어 데이터가 암호화 압축되면 도 5에 도시된 바와 같이, 멀티미디어 데이터 제공자는 멀티미디어 데이터 수신자(B)로부터 공용 키를 전송받고(1), 암호화 키(symmetric key 1, 2)는 멀티미디어 데이터 수신자(B)들의 공용 키로 암호화하여 전달한다(2).

<78> 멀티미디어 데이터 수신자들은 각자의 개인 키를 이용해 이를 복호화하여 멀티미디어 서비스를 통해 제공되는 압축된 멀티미디어 데이터를 복호화할 수 있게 된다.

<79> 즉, 본 발명에 따른 symmetric key 1, 2 및 r에 따라 멀티미디어 데이터를 인코딩하였기 때문에 symmetric key 1, 2값을 모른다면 복호화가 불가능하고 멀티미디어 데이터를 재생할 수 없으므로 보안성 제공이 가능한 것이다.

<80> 멀티미디어 제공자는 높은 보안성 유지를 위해 symmetric key 1, 2 및 r를 주기적으로 변경하게 되는데, r은 symmetric key 1, 2보다 자주 변경되어 r이 변경되는 시간(t)의 일정 배수보다 symmetric key 1, 2이 변경되는 시간(T)가 더 길다.

<81> 또한, 본 발명에 따른 암호화 압축하는 과정을 통해 AC 계수의 비트열이 줄어들어 압축율이 향상되는데, 상기 실시 예에서 symmetric key 2를 통해 인코딩하는 과정을 통해 AC 계수 (7,3)을 (7,2)로 변환됨으로써 AC 계수가 5비트 줄어드는 효과를 얻을 수 있다.

<82> 따라서, 8×8 블록이 하나의 프레임내 슬라이스 레이어(slice layer)의 macro block의 일부임을 고려할 때 전체 동영상 파일 크기에서는 상당한 압축 효과를 기대할 수 있다.

<83> 이러한 암호화 압축결과는 첨부된 도 6의 a,b,c와 7의 a,b,c를 통하여 설명하면, 도 6 및 7의 a는 원본 이미지를 나타내는 것이고, 도 6 및 7의 b는 두 원본 이미지를 암호화 압축한 결과를 나타낸 것이다.

<84> 이와 같이 암호화 압축된 이미지를 본 발명에 따른 symmetric key 1,2를 이용하여 복호화한 결과는 도 6 및 7의 c와 같다.

<85> 도 6 및 7의 c에 도시한 바와 같이, 본 발명에 따른 XOR 및 right shift와 같은 간단한 연산을 통해 효과적인 암호화 복호화 결과를 얻을 수 있게 되는 것이다.

<86> 또한, 도 6 및 7을 본 발명에 따라 암호화 압축한 결과에 따른 데이터 압축률을 기존의 압축률과 비교하면 표 5에 도시한 바와 같이 나타난다.

<87> 이를 통해 본 발명에 따른 압축률이 기존의 압축률에 비해 현저히 높은것을 확인할 수 있다.

<88> 【표 5】

	도 6		도 7	
	compression rate	size	compression rate	size
standard mpeg	81:1	31231(bytes)	40:1	174387
발명된 방법	118:1	21455	52:1	133968

<89> 그리고, 표 6은 해당 프레임을 계산하는데 걸린 오버헤드를 나타낸 것으로, 도 5의 경우에는 MPEG 표준에 따른 압축보다 0.05746초 더 소모되어 1.32%의 오버헤드를 나타내고, 도 6의 경우에는 0.039373초가 더 소모되어 0.88%의 추가적인 오버헤드가 필요하다.

<90> 이러한 결과를 통해 본 발명에 따라 발생되는 오버헤드가 무시할 정도로 적은 값임을 할 수 있다.

<91> 【표 6】

	도 6	도 7
standard mpeg	3.321732 (frame per second)	3.564230
발명된 방법	3.378378	3.603603

【발명의 효과】

<92> 본 발명에 따르면, 소정의 암호화 키에 따라 변화되는 엔트로피 인코딩 결과를 통해 입력되는 멀티미디어 데이터를 암호화 함으로써 암호화 및 복호화 과정이 복잡하지 않아 이동 단말기를 대상으로 하는 멀티미디어 서비스에 적합하며 압축효과가 크므로 무선 통신 상의 멀티미디어 처리에 효과적이다.

【특허청구범위】

【청구항 1】

입력되는 멀티미디어 데이터를 DCT에 적용시켜 DCT 계수를 생성하고, 생성된 DCT 계수를 양자화하는 단계와;

상기 양자화된 DCT의 DC 및 AC 계수를 엔트로피 인코딩할 때 소정의 암호화키에 따라 인코딩 결과를 변환시켜 변환된 DC 및 AC 계수를 암호화 압축하는 단계와;

상기 암호화된 DC 및 AC 계수를 허프만 테이블을 통해 허프만 부호화하여 출력하는 단계를 포함하는 것을 특징으로 하는 멀티미디어 암호화 압축방법.

【청구항 2】

제 1항에 있어서,

상기 DC 및 AC 계수를 암호화 압축하는 단계는

상기 DC 및 AC 계수에서 DC 계수는 DPCM하고 AC 계수는 런 랭스 코드화(run length coding)하는 단계;

상기 DPCM 및 런 랭스 코드화과정을 통해 얻어지는 상기 AC 및 DC 계수의 가변 길이 정보(VLC,VLI)를 이용하여 상기 AC 및 DC의 암호화 키 및 암호화 키의 시작 비트를 의미하는 랜덤 상수(r)를 결정하는 단계;

상기 결정된 암호화키를 이용해 상기 AC 및 DC 계수를 암호화하는 단계를 포함하는 것을 특징으로 하는 멀티미디어 암호화 압축방법.

【청구항 3】

제 2항에 있어서,

상기 DC 계수를 암호화하는 단계는

상기 결정된 DC의 암호화 키에서 상기 r번째 비트값이 1인지 여부를 판별하는 단계;

상기 판별결과 1이면 상기 DC 계수의 VLC값을 11111111과 배타적 논리합하여 상기DC 계수를 변환시키는 단계를 포함하는 것을 특징으로 하는 멀티미디어 암호화 압축방법.

【청구항 4】

제 2항에 있어서,

상기 AC 계수를 암호화하는 단계는

상기 결정된 암호화 키에서 상기 r번째 비트값이 1인지 여부를 판별하는 단계;

상기 판별결과 1이면 상기 AC 계수의 VLI를 오른쪽 편이(right shift)시키는 단계;

상기 오른쪽 편이된 VLI값을 통해 허프만 테이블을 이용하여 VLC를 결정하는 단계;

상기 결정된 VLC와 상기 VLI를 이용하여 상기 AC 계수를 변환시키는 단계를 포함하는 것을 특징으로 하는 멀티미디어 암호화 압축방법.

【청구항 5】

제 1항 내지 4항중 어느 한 항에 있어서,

상기 암호화 키는 대칭형 키(symmetric key)인 제 1 및 제 2 키이며 각각 상기 AC 및 DC의 VLC인 것을 특징으로 하는 멀티미디어 암호화 압축방법.

【청구항 6】

입력되는 멀티미디어 데이터를 이산 신호로 변환하여 AC 및 DC 계수로 이루어지는 DCT 계수를 생성하는 DCT와,

상기 DCT 계수를 양자화 테이블을 사용하여 양자화하는 양자화부와,

상기 양자화된 AC 및 DC 계수를 소정의 암호화키를 이용해 엔트로피 인코딩하여 AC 및 DC 계수를 암호화하는 엔트로피 암호화 인코딩부를 포함하는 것을 특징으로 하는 멀티미디어 암호화 압축장치.

【청구항 7】

제 6항에 있어서,

상기 엔트로피 암호화 인코딩부는 DCT 계수의 DC 계수를 펄스 변조하는 DPCM과,

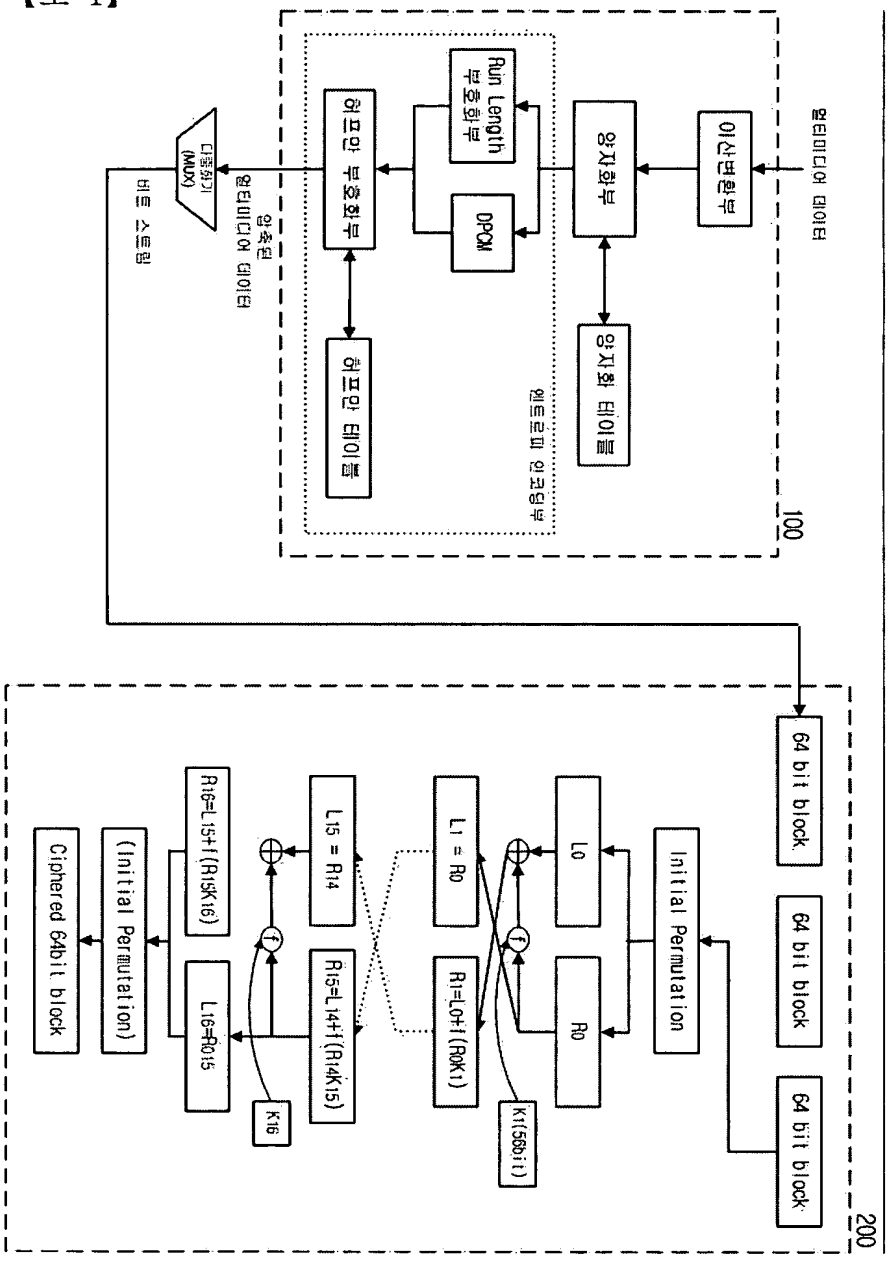
상기 DCT 계수의 AC 계수를 zig-zag run으로 스캔하는 런 랭스 부호화부와,

상기 DPCM과 런 랭스 부호화부를 통해 얻어지는 DC 및 AC 계수의 VLC 및 VLI를 이용하여 DC 및 AC를 암호화하는 암호화부와,

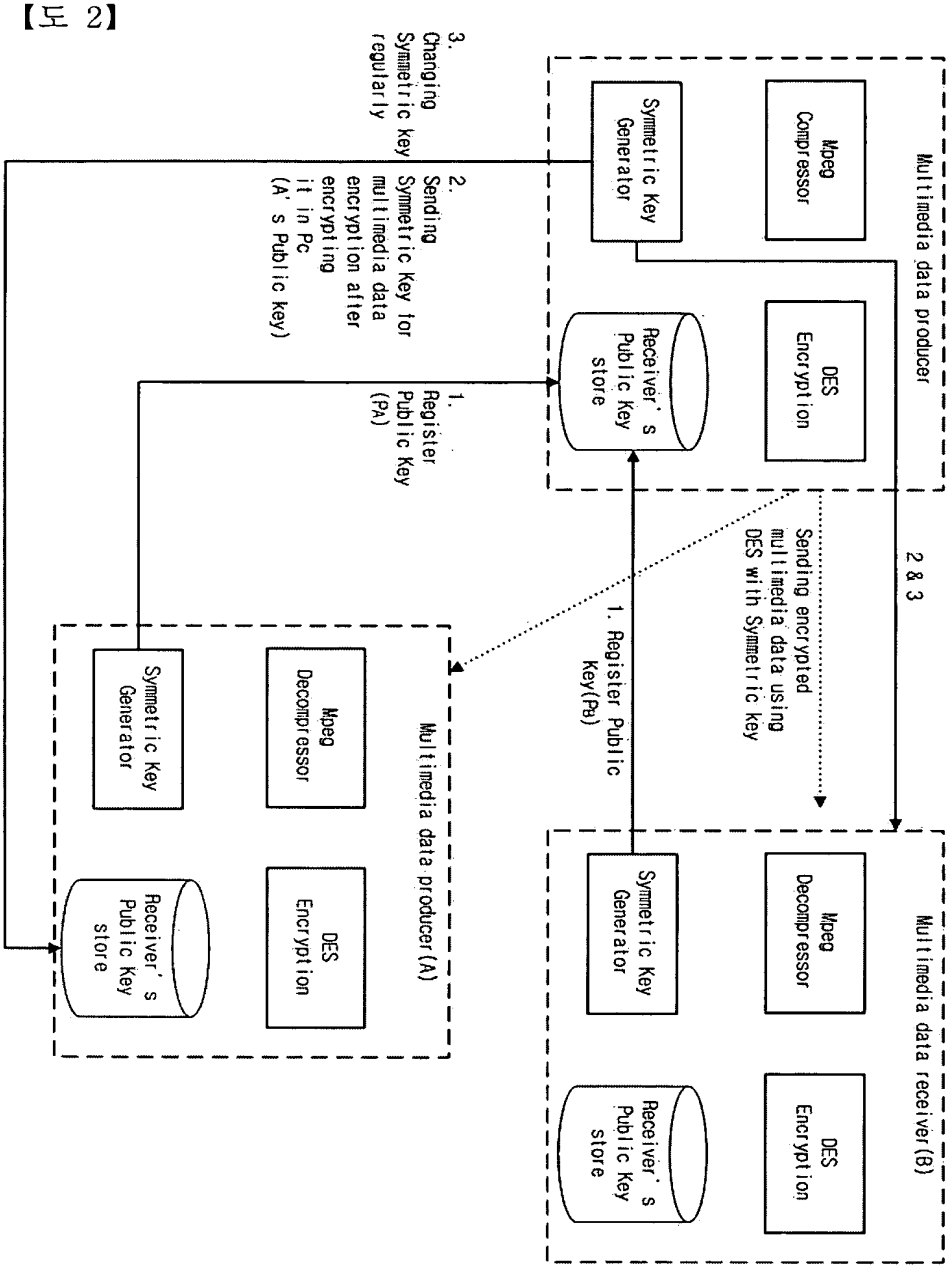
상기 암호화된 DC 및 AC를 허프만 테이블을 통해 허프만 부호화하는 허프만 부호화부를 포함하는 것을 특징으로 하는 멀티미디어 암호화 압축장치.

【도면】

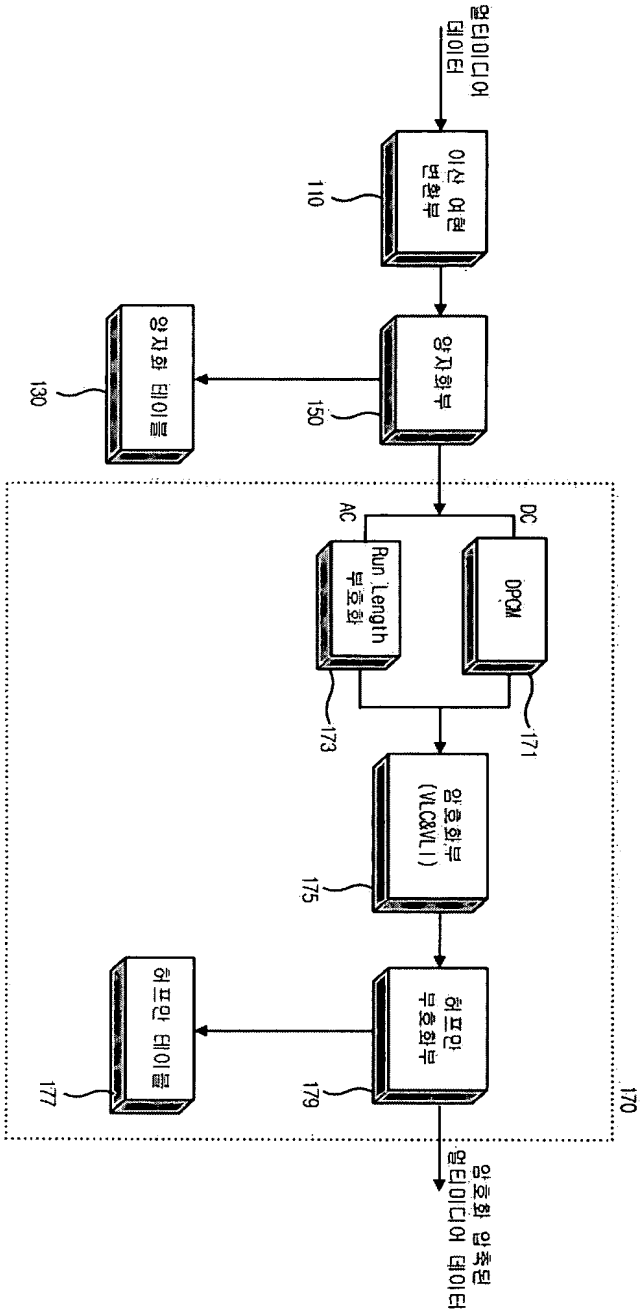
【도 1】


멀티미디어 데이터
이산변환부
양자화부
Run Length 부호화부
DPCM
허프만 부호화부
엔트로피 인코딩부
양자화 테이블
허프만 테이블
다중화기 (MUX)
압축된 멀티미디어 데이터
비트 스트림
100
64 bit block
64 bit block
64 bit block
Initial Permutation
L0
R0
L1 = R0
R1=L0+f(R0K1)
K1(56bit)
L15 = R14
R15=L14+f(R14K15)
K16
R16=L15+f(R15K16)
L16=R15
(Initial Permutation)
Ciphered 64bit block
200

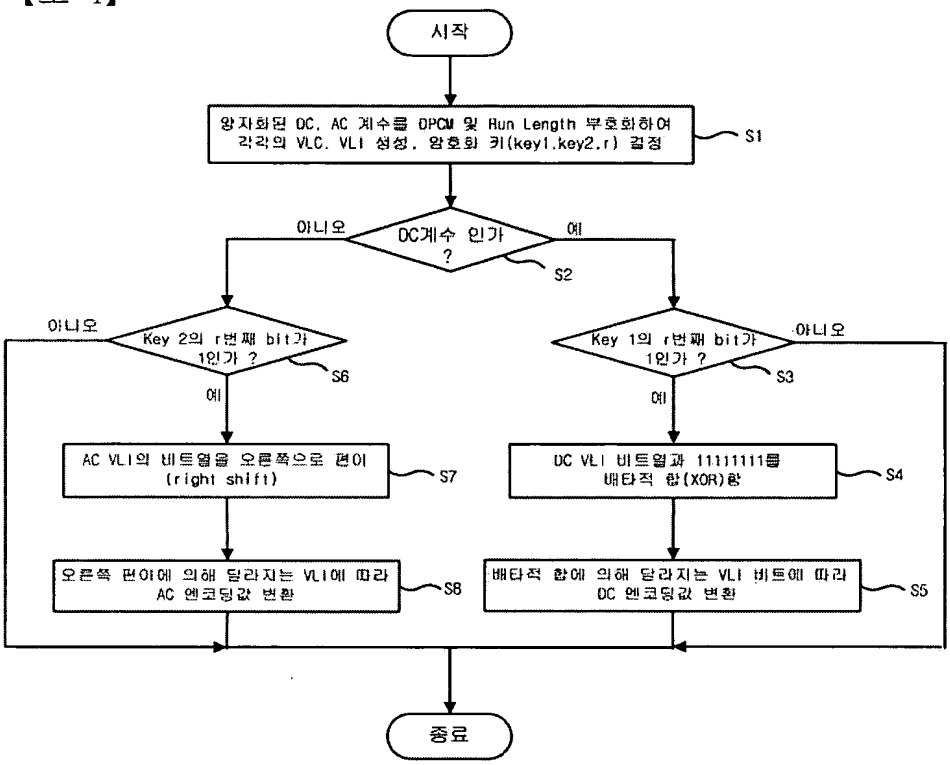
【도 2】


Multimedia data producer
Mpeg Compressor
Symmetric Key Generator
DES Encryption
Receiver's Public Key store
3. Changing Symmetric key regularly
2. Sending Symmetric Key for multimedia data encryption after encrypting it in Pc (A's Public key)
1. Register Public Key (PA)
Sending encrypted multimedia data using DES with Symmetric key
1. Register Public Key(PB)
2 & 3
Multimedia data receiver(B)
Mpeg Decompressor
Symmetric Key Generator
DES Encryption
Receiver's Public Key store
Multimedia data producer(A)
Mpeg Decompressor
Symmetric Key Generator
DES Encryption
Receiver's Public Key store

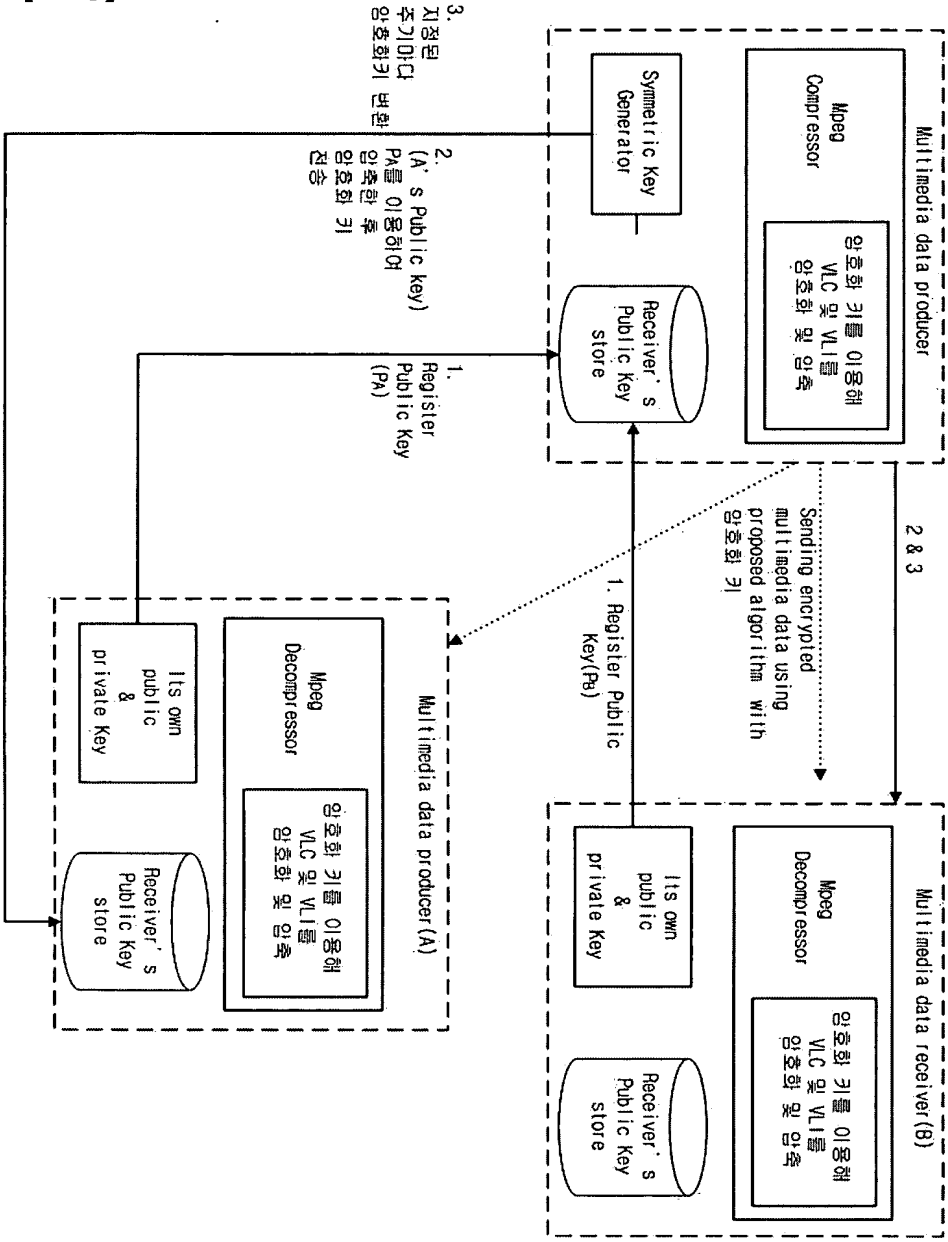
【도 3】


멀티미디어 데이터
이산 여현 변환부
110
양자화부
150
양자화 테이블
130
AC
DC
Run Length 부호화
DPCM
173
171
압축화부 (VLC&VLI)
175
허프만 부호화부
179
허프만 테이블
177
170
압축화 압축된 멀티미디어 데이터

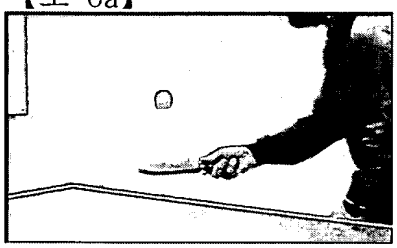
【도 4】


시작
양자화된 DC, AC 계수를 DPCM 및 Run Length 부호화하여 각각의 VLC, VLI 생성, 암호화 키(key1,key2,r) 결정
S1
DC계수 인가 ?
S2
아니오
예
Key 2의 r번째 bit가 1인가 ?
S6
Key 1의 r번째 bit가 1인가 ?
S3
AC VLI의 비트열을 오른쪽으로 편이 (right shift)
S7
DC VLI 비트열과 11111111를 배타적 합(XOR)함
S4
오른쪽 편이에 의해 달라지는 VLI에 따라 AC 엔코딩값 변환
S8
배타적 합에 의해 달라지는 VLI 비트에 따라 DC 엔코딩값 변환
S5
종료

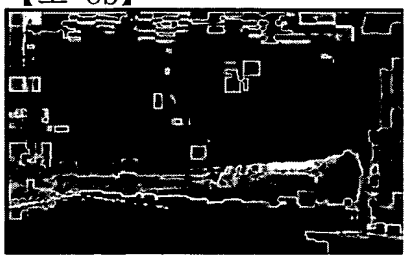
【도 5】


Multimedia data producer
Mpeg Compressor
암호화 키를 이용해 VLC 및 VLI를 암호화 및 압축
Symmetric Key Generator
Receiver's Public Key store
3. 지정된 주기마다 암호화키 변환
2. (A's Public key) PA를 이용하여 암호화한 후 암호화 키 전송
1. Register Public Key (PA)
Sending encrypted multimedia data using proposed algorithm with 암호화 키
1. Register Public Key(PB)
2 & 3
Multimedia data receiver(B)
Mpeg Decompressor
암호화 키를 이용해 VLC 및 VLI를 암호화 및 압축
Its own public & private Key
Receiver's Public Key store
Multimedia data producer(A)
Mpeg Decompressor
암호화 키를 이용해 VLC 및 VLI를 암호화 및 압축
Its own public & private Key
Receiver's Public Key store

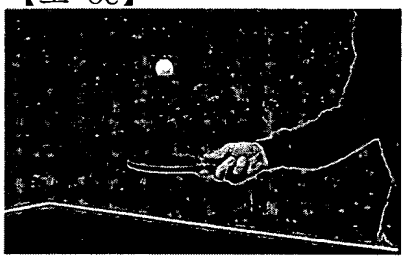
【도 6a】



【도 6b】

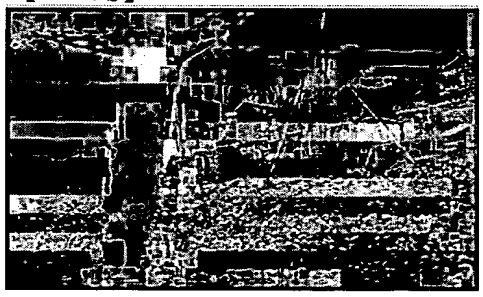


【도 6c】



【도 7a】

【도 7b】



【도 7c】